Title (en)

Method and server for providing transaction keys

Title (de)

Verfahren und Server zur Bereitstellung von Transaktionsschlüsseln

Title (fr)

Procédé et serveur pour fournir des codes de transaction

Publication

EP 3021516 A1 20160518 (EN)

Application

EP 14003796 A 20141111

Priority

EP 14003796 A 20141111

Abstract (en)

A method and a server for providing transaction keys for a transaction system are improved. Transaction units of the transaction system use pre-delivered transaction keys, which are provided by a key provisioning server and wherein the transaction key usage is checked by a transaction checking server. A transaction key is derived from a master key of a transaction unit, wherein a varying derivation parameter is used in the step of deriving. The step of deriving comprises a first sub step (12) of deriving a key from the master key and a second sub step (14) of deriving the transaction key from the derived key. The first sub step (12) or the second sub step (14) of deriving is performed dependent on a security level of the transaction unit.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/32** (2006.01); **H04L 29/06** (2006.01)

CPC (source: EP US)

H04L 9/0822 (2013.01 - EP US); **H04L 9/0863** (2013.01 - EP US); **H04L 9/3228** (2013.01 - EP US); **H04L 63/062** (2013.01 - EP US); **H04L 63/067** (2013.01 - EP US); **H04L 63/105** (2013.01 - EP US); H04L 63/126 (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US); H04L 2463/062 (2013.01 - EP US)

Citation (applicant)

WO 2013050153 A1 20130411 - GIESECKE & DEVRIENT GMBH [DE]

Citation (search report)

- [XI] WO 2010010430 A2 20100128 - KOK-WAH LEE [MY]
- [AD] WO 2013050153 A1 20130411 - GIESECKE & DEVRIENT GMBH [DE]
- [A] US 2009222383 A1 20090903 - TATO CHARLES [US], et al
- [A] WO 0106701 A1 20010125 - SUDIA FRANK W [US]

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 3021516 A1 20160518; US 10396989 B2 20190827; US 2017324560 A1 20171109; WO 2016074781 A1 20160519

DOCDB simple family (application)

EP 14003796 A 20141111; EP 2015002245 W 20151109; US 201515525717 A 20151109